Theoretical Computer Science 47 (1986) 335-343
North-Holland

NOTE

THE RATIONAL INDEX OF THE DYCK LANGUAGE $D_1'^*$

Jean-Luc DELEAGE
Université de Dijon U.E.R.-M.I.P.C. et L.I.T.P., 21004 Dijon Cedex, France

Laurent PIERRE
Université de Paris X Nanterre, 92001 Nanterre Cedex, France

Communicated by M. Nivat
Received March 1984
Revised March 1986

Key words. Formal language theory, rational index, Dyck language.

1. Introduction

In order to measure the complexity of languages, the rational index was introduced by Boasson and Nivat in [1]. The rational index of a nonempty language L is a function ρ_L of $\mathbb{N}-\{0\}$ into $\mathbb{N}$. The asymptotical behaviour of this function allows to classify languages [2, 3, 4]. More precisely, let n be a positive integer. For each rational language K recognized by a finite nondeterministic automaton with n states and not disjoint with L, let us consider $\delta_{L\cap K}$: the length of a shortest word in $L\cap K$. Then $\rho_L(n)$ is the maximum of $\delta_{L\cap K}$ for all such K.

On the other hand, the restricted Dyck language $D_1'^*$ is the set of all well-parenthesized words in $\{a, b\}^*$, considering a and b respectively as left and right parentheses. Then Boasson, Courcelle, and Nivat have shown [2] that $O(n^2)\leqslant \rho_{D_1'^*}(n)\leqslant O(n^3)$ and conjectured that $\rho_{D_1'^*}(n)=O(n^2)$, which we shall prove here.

2. Definitions

- $\lfloor x\rfloor$ will denote the integral part of a real number x.
- $x\equiv y\,[m]$ means that x and y are congruent modulo m.
- Throughout this paper the expressions *less*, *negative*, *positive*, *shorter*, and *higher* are understood *strictly*.
- $|w|$ will denote the length of a word w.
- $\mathrm{Rat}_n(X)$ will denote the set of regular languages on an alphabet X, recognized by a finite nondeterministic automaton with at most n states.

0304-3975/86/$3.50

- Let L be a language on the alphabet X. The rational index of L is the function ρ_L of $\mathbb{N}-\{0\}$ into $\mathbb{N}$ defined by the formula

$$\rho_L(n)=\max\{\min\{|w|: w\in L\cap K\}, K\in \mathrm{Rat}_n(X), L\cap K\neq\emptyset\}.$$

- Let x be in X and w be a word in X^*. $|w|_x$ will denote the number of occurrences of the letter x in w.
- A word f in X^* is a prefix (respectively suffix) of w if $fg=w$ (respectively $gf=w$) for some g *in* X^*.
- PR(L) (respectively SU(L)) will denote the set of all the prefixes (respectively suffixes) of words in L.
- Let $w\in\{a, b\}^*$. The height of w is the difference between the number of a's and the number of b's in w: $h(w)=|w|_a-|w|_b$.
- The restricted Dyck language $D_1'^*$ is the context-free language generated by the grammar $G=\langle\{a, b\}; \{S\}; S; \{S\to aSbS+\varepsilon\}\rangle$. $D_1'^*$ is the set of all well-parenthesized words, i.e., of all words w in $\{a, b\}^*$, such that
  (1) $h(w)=0$,
  (2) for any prefix f of w, $h(f)\geqslant 0$.
- A word u is called a subword of a word v if $u=x_1x_2\ldots x_n$ and $v=y_0x_1y_1x_2y_2\ldots y_{n-1}x_ny_n$ for some n and some words $y_0, x_1, y_1, x_2, y_2\ldots y_{n-1}, x_n$, and y_n.
- A path in an automaton from a state q to a state q' is called a loop if $q=q'$.
- A path u is called a subpath of a path v if $u=x_1x_2\ldots x_n$ and $v=y_0x_1y_1x_2y_2\ldots y_{n-1}x_ny_n$ for some n, some paths $x_0, x_1,\ldots, x_n, y_0, y_n$ and some loops $y_1, y_2,\ldots, y_{n-1}$. Then the label of u is a subword of the label of v.
- The height of a path is the height of its label.
- The height of a particular state in a path is the height of the prefix of this path ending at this state.
- A simple loop is a nonempty loop that does not go twice through the same state.
- A path or a loop is said to be positive, negative, or null according to its height.
- A path x is called an upper (respectively lower) subpath of a path y if $x=x_1x_2\ldots x_n$ and $y=y_0x_1y_1x_2y_2\ldots y_{n-1}x_ny_n$ for some n, some paths $x_1, x_2,\ldots, x_n, y_0, y_n$ and some nonpositive (respectively nonnegative) loops $y_1, y_2,\ldots, y_{n-1}$.
- A subpath that is a loop is called a subloop.
- From the definitions it is obvious that if x is a subpath of a subpath of y, then x is a subpath of y. And similarly, if x is an upper subpath of an upper subpath of y, then x is an upper subpath of y.

3. Lower bound of $\rho_{D_1'^*}(n)$

We state that $\rho_{D_1'^*}(n)\geqslant\lfloor\frac{1}{2}(n+1)^2\rfloor-2$. To prove this we only have to build an automaton $\mathfrak{A}$ with n states, accepting a regular language K such that the length of a shortest word in $D_1'^*\cap K$ is $\lfloor\frac{1}{2}(n+1)^2\rfloor-2$.

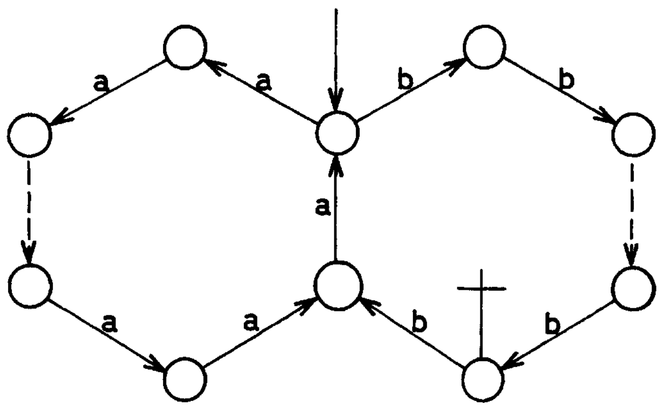

Fig. 1.

Case 1: n is odd ($n>1$). Let $\mathfrak{A}$ be as is shown in Fig. 1, with $\frac{1}{2}(n+1)$ edges labelled a and $\frac{1}{2}(n+1)$ edges labelled b. Let w be in $D_1'^* \cap K$. The path in $\mathfrak{A}$ accepting w is a mixture of λ times the left loop labelled $a^{(n+1)/2}$, μ times the right loop labelled $b^{(n+1)/2}a$, and once the direct path labelled $b^{(n-1)/2}$ from the initial state to the final state. Thus:

$$|w| = \lambda\tfrac{1}{2}(n+1) + \mu\tfrac{1}{2}(n+3) + \tfrac{1}{2}(n-1),$$

$$h(w) = \lambda\tfrac{1}{2}(n+1) - \mu\tfrac{1}{2}(n-1) - \tfrac{1}{2}(n-1) = 0.$$

This last relation rewrites $\lambda\frac{1}{2}(n+1) = (\mu+1)\frac{1}{2}(n-1)$. Since $\frac{1}{2}(n-1)$ and $\frac{1}{2}(n+1)$ are two consecutive integers, they are relatively prime. Hence $\lambda = \nu\frac{1}{2}(n-1)$ and $\mu+1 = \nu\frac{1}{2}(n+1)$ for some $\nu \in \mathbb{N}-\{0\}$. Hence, $|w| = \nu\frac{1}{2}(n+1)^2 - 2$. Thus we have proved that if w is in $D_1'^* \cap K$, then its length is at least $\frac{1}{2}(n+1)^2 - 2$. Conversely, by setting $\nu = 1$, we can get $w_0 = (a^{(n+1)/2})^{(n-1)/2}(b^{(n+1)/2}a)^{(n-1)/2}b^{(n-1)/2}$. w_0 is in $D_1'^* \cap K$ and $|w_0| = \frac{1}{2}(n+1)^2 - 2$. Hence, w_0 is a shortest word in $D_1'^* \cap K$.

Case 2: n is even ($n>2$). Let $\mathfrak{A}$ be as is shown in Fig. 2, with $\frac{1}{2}n$ edges labelled a and $\frac{1}{2}n+1$ edges labelled b. In a similar way we can prove that if w is in $D_1'^* \cap K$, then $|w| = \nu\lfloor\frac{1}{2}(n+1)^2\rfloor - 2$ for some $\nu \in \mathbb{N}-\{0\}$, and that $w_0 = a^{n/2(n/2+1)-1}b^{n/2(n/2+1)-1}$ is a shortest word in $D_1'^* \cap K$.

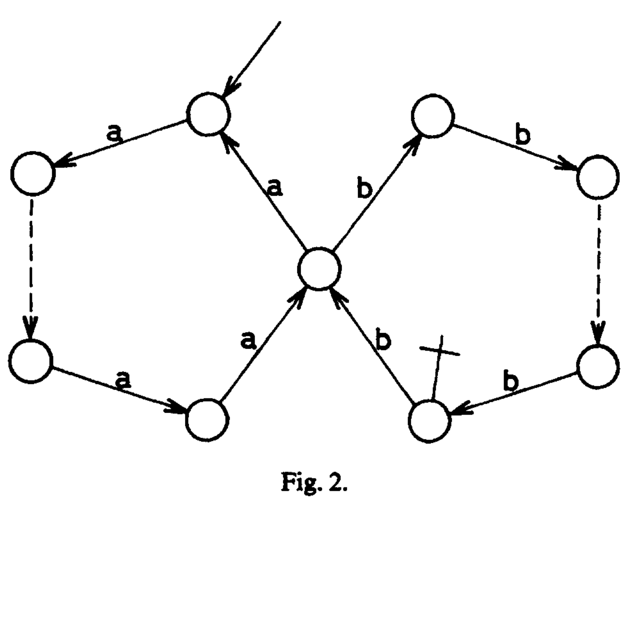

Fig. 2.

4. Method used to bound $\rho_{D_1'^*}(n)$

Let $n \in \mathbb{N} - \{0\}$ be fixed. We shall prove that $\rho_{D_1'^*}(n) \leq 2n^2 + 4n$. Let $\mathfrak{A}$ be a nondeterministic finite automaton with n states accepting K such that $D_1'^* \cap K \neq \emptyset$. Let w be a shortest word in $D_1'^* \cap K$. If $|w| \geq n^2$, then, using w, we shall build a word $w' = \alpha u^\lambda \beta v^\mu \gamma$ in $D_1'^* \cap K$ such that:

- $\alpha\beta\gamma$ and $\alpha u v \gamma$ are subwords of w,
- $0 \leq h(\alpha) < n$,
- $-n < h(\gamma) \leq 0$,
- $|u| \leq n$, $h(u) > 0$,
- $|v| \leq n$, $h(v) < 0$,
- $p = \gcd(h(u), -h(v))$,
- $|\alpha\beta\gamma| \leq n(p+2)$,
- $h(\alpha\beta\gamma) \equiv 0[p]$,
- $\alpha u^* \beta v^* \gamma \subset K$,
- $\alpha u^* \subset \mathrm{PR}(D_1'^*)$,
- $v^* \gamma \subset \mathrm{SU}(D_1'^*)$.

We shall first define u and v, and then α, β, and γ. Then we shall define λ and μ as the least integers making sure that $w' \in D_1'^*$. At last we shall prove that $\lambda + \mu + p \leq 2n + 2$. Hence,

$$|w'| \leq |\alpha\beta\gamma| + \lambda|u| + \mu|v| \leq (p+2)n + \lambda n + \mu n \leq 2n^2 + 4n.$$

5. Arithmetical lemmas

Lemma 1. *Let $p \in \mathbb{N} - \{0\}$. Let $m_1, m_2, \ldots, m_p \in \mathbb{Z}$. Then there exist k $(k \geq 1)$ of these numbers such that $m_{i_1} + m_{i_2} + \cdots + m_{i_k} \equiv 0\,[p]$.*

Proof. Let $s_i = \sum_{j=1}^{i} m_j$ for $i = 1, 2, \ldots, p$ and $s_0 = 0$. At least two of these $p+1$ numbers have the same residues modulo p. Let s_i and s_k (with $i < k$) be two such numbers. Then we have $\sum_{j=i+1}^{k} m_j = s_k - s_i \equiv 0\,[p]$. $\square$

Lemma 2. *Let t, s, m and M be four real numbers such that $s > 0$ and $0 < m \leq t \leq M$. Then $t + s/t \leq \max(m + s/m,\ M + s/M)$.*

Proof. Let us consider the function $[m, M] \to \mathbb{R} : t \mapsto t + s/t$. Since it is convex, it reaches its maximum at the bounds of $[m, M]$. $\square$

This lemma will be used in a few cases:

- if $1 \leq x \leq n$, then $x + n/x \leq n + 1$;
- if $2 \leq x \leq n$, then $x + 2n/x \leq n + 2$;
- if $1 \leq x$, $1 \leq y$, and $xy \leq n$, then $x + y \leq n + 1$.

6. Construction of α, u, β, v and γ

From now on we shall use the notation of Section 4. We shall also identify a path and its label. Let c be a path in $\mathfrak{A}$ from the initial state to a final state labelled by w.

Lemma 3. *Two occurrences of a same state q in c have different heights.*

Proof. If a state q appears twice in c with the same heights, then the loop between these two occurrences has height 0 and may be removed, giving a path shorter than c labelled by a word in $D_1'^* \cap K$. This is a contradiction since w is a shortest word in $D_1'^* \cap K$. □

Lemma 4. *If $|w| \geq n^2$, then c contains a state with a height greater than or equal to n.*

Proof. By Lemma 3 there are at most n^2 states in c with a height less than n. Since c has at least n^2+1 states, the result holds. □

Lemma 5. *If x is a path in $\mathfrak{A}$ such that $h(x) \geq n$, then x has a positive upper subloop.*

Proof. The last state of x has a height greater than or equal to n. Hence, x has states with heights $0, 1, \ldots, n$. Let q_i be the first state in x with height i, for $i = 0, 1, \ldots, n$. $q_0, q_1, \ldots, q_n$ are in this order in x. Two of these $n+1$ states are equal. The loop between them is positive and it is an upper subloop of x. □

Lemma 6. *Any positive loop has a positive simple upper subloop.*

Proof. We shall prove it by induction on the length of the loop. Let x be a positive loop. Let us assume that any positive loop shorter than x has a positive simple upper subloop. If x is simple, then x is the subloop. If x is not simple, then it goes twice through a state q and x can be split in three parts y, z, and t,

$$x : r \xrightarrow{y} q \xrightarrow{z} q \xrightarrow{t} r,$$

such that the two loops yt and z are nonempty and shorter than x. If z is positive, then using the induction hypothesis we can find a simple positive upper subloop of z, and hence of x. If z is not positive, then yt is a positive (for yt is higher than or as high as x) upper subloop of x. Using the induction hypothesis we can find a simple positive upper subloop of yt, and hence of x. □

By combining Lemmas 5 and 6 we can state the following lemma.

Lemma 7. *If x is a path in $\mathfrak{A}$ such that $h(x) \geqslant n$, then x has a positive simple upper subloop.*

6.1. Construction of u and v

Since $|w| \geqslant n^2$, by Lemma 4 we have $c = c'c''$, where $h(c') \geqslant n$ and $h(c'') \leqslant -n$. By Lemma 7 we know that c' has a simple positive upper subloop. Let u be the leftmost such subloop, i.e., the simple positive upper subloop of c' starting at the leftmost state in c'. Let α' be the part of c' preceding this state. In other words, α' is the least prefix of c' such that $c' = \alpha' x_1 y_1 x_2 y_2 \ldots x_k y_k$, $u = x_1 x_2 \ldots x_k$ is a simple positive loop, and $y_1, \ldots, y_{k-1}$ are nonpositive loops. (N.B. x_1 may be empty.)

Similarly, we define v as the rightmost simple negative lower subloop of c'' and γ' as the suffix of c'' starting at the last state of v. α' is a prefix of c' and γ' is a suffix of c''. Hence, they do not overlap in c. Let β' be such that $\alpha'\beta'\gamma' = c$.

We shall now build α, β, and γ by removing loops out of α', β', and γ'. Let $p = \gcd(h(u), -h(v))$. Let us define the finite sequence $(\alpha_i, \beta_i, \gamma_i)$ by induction in the following way.

- $(\alpha_0, \beta_0, \gamma_0) = (\alpha', \beta', \gamma')$.
- If $\lfloor |\alpha_i|/n \rfloor + \lfloor |\beta_i|/n \rfloor + \lfloor |\gamma_i|/n \rfloor < p$, then $(\alpha_i, \beta_i, \gamma_i)$ is the last term of the sequence.
- If $\lfloor |\alpha_i|/n \rfloor + \lfloor |\beta_i|/n \rfloor + \lfloor |\gamma_i|/n \rfloor \geqslant p$, then looking at the n first edges and then at the n following edges and so on of α_i, β_i, and γ_i we can find $\lfloor |\alpha_i|/n \rfloor$ loops in α_i, $\lfloor |\beta_i|/n \rfloor$ loops in β_i, and $\lfloor |\gamma_i|/n \rfloor$ loops in γ_i. Thus we get at least p disjoint loops. According to Lemma 1, we can choose some of these loops so that the sum of their heights is divisible by p. We remove these loops out of α_i, β_i, and γ_i and we get α_{i+1}, β_{i+1}, and γ_{i+1}.

Since the length of $\alpha_i\beta_i\gamma_i$ decreases at each step, the sequence is finite. Thus we define (α, β, γ) as the last term of this sequence.

We now have to prove that α, β, and γ have the properties stated in Section 4.

- Since $h(\alpha'\beta'\gamma') = 0$ and since, at each step, we have $h(\alpha_i\beta_i\gamma_i) \equiv h(\alpha_{i+1}\beta_{i+1}\gamma_{i+1})$ $[p]$, it follows that $h(\alpha\beta\gamma) \equiv 0$ $[p]$.
- We have $\lfloor |\alpha|/n \rfloor + \lfloor |\beta|/n \rfloor + \lfloor |\gamma|/n \rfloor \leqslant p - 1$, hence,

$$
\begin{aligned}
|\alpha\beta\gamma| &\leqslant n\left(\left\lfloor \frac{|\alpha|}{n} \right\rfloor + 1\right) + n\left(\left\lfloor \frac{|\beta|}{n} \right\rfloor + 1\right) + n\left(\left\lfloor \frac{|\gamma|}{n} \right\rfloor + 1\right) \\
&\leqslant 3n + n\left(\left\lfloor \frac{|\alpha|}{n} \right\rfloor + \left\lfloor \frac{|\beta|}{n} \right\rfloor + \left\lfloor \frac{|\gamma|}{n} \right\rfloor\right) \\
&\leqslant 3n + n(p-1) \leqslant n(p+2).
\end{aligned}
$$

We can also see that $|\beta| \leqslant n(\lfloor |\beta|/n \rfloor + 1) \leqslant np$.

Lemma 8. *All the loops removed out of the α_i's are nonpositive.*

Proof. Let us assume the contrary. Let j be the least integer such that α_j contains a positive loop. Therefore, $\alpha_0, \alpha_1, \ldots$, and α_{j-1} contain no positive loops, and α_j has been obtained from α' by removing nonpositive loops. Thus it is an upper subpath of α'. Hence, the positive loop in α_j is a positive upper subloop of α'. Lemma 6 tells us that α' has a positive simple upper subloop, which is then at the left of u in c. But u was chosen as the leftmost simple upper subloop of c. This is a contradiction. □

Lemma 9. $h(\alpha) < n$.

Proof. Let us suppose that $h(\alpha) \geqslant n$. By Lemma 7, α has a positive simple upper subloop, which is also an upper subloop of α' since, by Lemma 8, α is an upper subpath of α'. We conclude as in the previous proof. □

Lemma 10. $\alpha u^* \subset \mathrm{PR}(D_1'^*)$.

Proof. By removing nonpositive loops, α' gives α and some prefix of c' gives $\alpha' u$, hence this prefix of c' gives αu. Hence, all the states in αu have heights at least equal to the (nonnegative) heights of the corresponding states in c'. Hence, their heights are nonnegative and $\alpha u \in \mathrm{PR}(D_1'^*)$. Since $h(u) > 0$, we can state that $\alpha u^* \subset \mathrm{PR}(D_1'^*)$. □

Thus $0 \leqslant h(\alpha) < n$. u is a positive simple loop, hence $0 < h(u) \leqslant |u| \leqslant n$. Similarly, we can prove that $-n < h(\gamma) \leqslant 0$, $0 < -h(v) \leqslant |v| \leqslant n$, and $v^*\gamma \subset \mathrm{SU}(D_1'^*)$. By the construction it is obvious that $\alpha u^* \beta v^* \gamma \subset K$.

7. Construction of λ and μ

From now on we shall consider α, u, β, v, and γ only as words and no longer as paths. Let $x = h(u)$ and $y = -h(v)$. Recall that $p = \gcd(x, y)$. Let $x' = x/p$ and $y' = y/p$. Let $w' = \alpha u^\lambda \beta v^\nu \gamma$. We want

$$h(w') = h(\alpha\beta\gamma) + \lambda x - \mu y = 0. \tag{1}$$

Since $h(\alpha\beta\gamma)$ is multiple of p, this equation is solvable in $\mathbb{Z}$, and the solutions are

$$\lambda = \lambda_0 + y'\nu, \qquad \mu = \mu_0 + x'\nu, \tag{2}$$

where (λ_0, μ_0) is a particular solution and ν is any integer. We must choose ν large enough so that λ and μ are nonnegative. Let $s = h(\alpha) + \lambda x - |\beta|_b$. Using (1) and (2), s can be written as

$$s = |h(\gamma)| + \mu y - |\beta|_a = s_0 + x'y'p\nu$$

for some s_0.

Lemma 11. *If ν is such that $\lambda \geqslant 0$, $\mu \geqslant 0$, and $s \geqslant 0$, then w' is in $D_1'^*$.*

Proof. We know that $h(w') = 0$. We have to show that any prefix of w' is nonnegative. Let $w' = fg$. According to the location of the cut in w', we have three cases.

Case 1: If f is a prefix of αu^λ, then, by Lemma 10, $h(f) \geqslant 0$.

Case 2: If $f = \alpha u^\lambda f'$ where f' is a prefix of β, then $h(f') \geqslant -|f'|_b \geqslant -|\beta|_b$ hence $h(f) \geqslant s \geqslant 0$.

Case 3: If $f = \alpha u^\lambda \beta f'$ where f' is a prefix of $v^\mu \gamma$, then g is a suffix of $v^\mu \gamma$. Hence, $h(g) \leqslant 0$ and $h(f) = -h(g) \geqslant 0$. $\square$

Since x', y' and $x'y'p$ are positive, λ, μ, and s are nonnegative if ν is large enough. We choose ν minimal such that $\lambda \geqslant 0$, $\mu \geqslant 0$, and $s \geqslant 0$. If instead of ν we would have taken $\nu - 1$, then λ, μ, and s would have been replaced by $\lambda - y'$, $\mu - x'$, and $s - x'y'p$. Hence, at least one of these three numbers is negative. Let us show that in each of the three resulting cases, $\lambda + \mu + p \leqslant 2n + 2$. (We shall use Lemma 2 in each case.)

Case 1: $\lambda - y' < 0$. Then $\lambda \leqslant y' - 1$; $h(\alpha) \leqslant n$, $h(\gamma) \leqslant 0$, and $h(\beta) \leqslant |\beta| \leqslant pn$, hence $h(\alpha\beta\gamma) \leqslant np + n$.

$$\mu = \frac{\lambda x + h(\alpha\beta\gamma)}{y} \leqslant \frac{\lambda x'}{y'} + \frac{np + n}{py'}.$$

(a) If $y' = 1$, then $\lambda = 0$, and we have

$$\mu \leqslant n + \frac{n}{p},$$

$$\lambda + \mu + p \leqslant n + \left(\frac{n}{p} + p\right) \leqslant n + (n+1) = 2n + 1.$$

(b) If $y' \geqslant 2$, then

$$\mu \leqslant x' + \frac{n}{y'} + \frac{n}{py'} \leqslant x' + \frac{2n}{y'},$$

$$\lambda + \mu + p \leqslant (y' - 1) + \left(x' + \frac{2n}{y'}\right) + p \leqslant (x' + p) + \left(y' + \frac{2n}{y'}\right) - 1$$

$$\leqslant (n+1) + (n+2) - 1 = 2n + 2.$$

Case 2: $\mu - x' < 0$. This case is similar to the first case.

Case 3: $s - x'y'p < 0$. Then $s < x'y'p$.

$$\lambda = \frac{s - h(\alpha) + |\beta|_b}{x} \leqslant \frac{x'y'p + |\beta|_b}{x} = y' + \frac{|\beta|_b}{x},$$

$$\mu = \frac{s - |h(\gamma)| + |\beta|_a}{y} \leqslant \frac{x'y'p + |\beta|_a}{y} = x' + \frac{|\beta|_a}{y},$$

$$\lambda + \mu + p \leqslant y' + x' + \frac{|\beta|_a}{y} + \frac{|\beta|_b}{x} + p,$$

(a) If $x \leqslant y$, then we have

$$\frac{|\beta|_a}{y} \leqslant \frac{|\beta|_a}{x},$$

$$\begin{aligned}\lambda + \mu + p &\leqslant y' + x' + \frac{|\beta|_a + |\beta|_b}{x} + p \\ &\leqslant y' + x' + \frac{np}{x} + p = \left(x' + \frac{n}{x'}\right) + (y' + p) \\ &\leqslant (n+1) + (n+1) = 2n + 2.\end{aligned}$$

(b) $y \leqslant x$. This case is similar to the previous one.

Hence, we have built a word w' in $D_1'^* \cap K$ such that $|w'| \leqslant 2n^2 + 4n$. The proof that $\rho_{D_1'^*}(n) \leqslant 2n^2 + 4n$ is complete.

References

[1] L. Boasson and M. Nivat, Ordres et types de langage, I, II, III, Notes CRAS, Série A tome 284 (1977) 559-562, 625-628, 703-705.

[2] L. Boasson, B. Courcelle and M. Nivat, A new complexity measure, *Proc. Conf. on Theoretical Computer Science*, Waterloo, Ontario (1977) 130-138.

[3] L. Boasson, B. Courcelle and M. Nivat, The rational index, a complexity measure for languages, *SIAM J. Comput.* **10**(2) (1981) 284–296.

[4] J. Gabarro, Index rationnel, centre et langages algébriques, Thèse de 3ième cycle, Univ. de Paris VI, Rapport L.I.T.P. No. 81-54 (1981).